BLACK BOX NETWORK SERVICES

LVN5200A-R2
LVN5250A-R2
LVN5400A-R2
LVN5600A-R2
LVN5800A-R2

Veri-NAC™ Frequently Asked Questions (FAQs)

Veri-NAC—the fastest to deploy, easiest to use Network Access Control (NAC) appliance for Intrusion Prevention, Vulnerability Management, and Regulatory Compliance.

Black Box answers your technical questions.

Trademarks Used in this Document

Black Box and the Double Diamond logo are registered trademarks, and Veri-NAC is a trademark, of BB Technologies, Inc.

CA-Unicenter is a registered trademark of Computer Associates International.

HP and OpenView are registered trademarks of Hewlett-Packard Company.

IBM and Tivoli are registered trademarks of International Business Machines Corporation.

Juniper Networks and NetScreen are registered trademarks of Juniper Networks, Inc.

Cisco is a trademark of Cisco Technology, Inc.

Check Point is a registered trademark of Check Point Software Technologies Ltd.

Windows, Excel, and Internet Explorer are registered trademarks of Microsoft Corporation.

Firefox is a registered trademark of Mozilla Foundation.

Linux is a registered trademark of Linux Torvalds.

Unix is a registered trademark of X/Open Company.

Any other trademarks mentioned in this document are acknowledged to be the property of the trademark owners.

Table of Contents

1. Deployment Guide **3**
2. General Use **4**
3. Advanced Use **7**
4. Managed Switch and Firewall **9**
5. Audits **10**
6. Workflow/Ticket Management **11**
7. Policies, Regulations, and Reports **12**
8. Backup and Restore **13**
9. Command Center **15**
10. New Features in Veri-NAC Version 8.0 ..... **17**
11. Troubleshooting the Veri-NAC Blocking Engine **21**

1. Deployment Guide

QUESTION: What are the roles of NAC users?

ANSWER: NAC users can only access Network Access Control functionality and are not involved in vulnerability remediation. This means that they can access Setup, Network Access Control, System, and Asset Tracker in the sidebar.

QUESTION: What are the roles of IT staff users?

ANSWER: IT staff users work with managers on vulnerability remediation. They can select jobs they want to work on (or have jobs assigned to them), change a job status to "To be Confirmed," or tag a vulnerability as a potential false positive. They can also access all network access control functionality available to NAC Users.

QUESTION: What are the roles of managers?

ANSWER: Managers control all users assigned to them in the hierarchy. They can assign work to themselves or anyone in their group, regardless of other manager levels existing within the group (there can easily be multiple levels of Managers). Managers can modify time allocated for remediation of vulnerabilities at different risk levels, assign tasks to other users, confirm false positives, and close jobs. Managers can access and create all types of reports and add or remove any sub-manager, IT staff user, or NAC user beneath them in the hierarchy.

NOTE: MainAccount is always the highest-level manager, and there can be only one.

QUESTION: In my large network, I intend to have Veri-NAC appliances for each segment. Is there way to centrally control all these Veri-NAC appliances? Do they share a common trusted MAC list? Can they share the same policy set?

ANSWER: Managers control all users assigned to them in the hierarchy. They can assign work to themselves or anyone in their group, regardless of other manager levels existing within the group (there can easily be multiple levels of Managers). Managers can modify time allocated for remediation of vulnerabilities at different risk levels, assign tasks to other users, confirm false positives, and close jobs. Managers can access and create all types of reports and add or remove any sub-manager, IT staff user, or NAC user beneath them in the hierarchy.

QUESTION: We have multiple subnets in our networks (local and remote). How should we deploy Veri-NAC?

ANSWER: You should deploy one Veri-NAC LVN5400A-R2, LVN5600A-R2, or LVN5800A-R2 unit in your data center or main rack at the IT headquarters subnet. Veri-NAC LVN5200A-R2 or LVN5250A-R2 units, which are centrally manageable using the built-in Command Center running in your LVN5400A-R2, LVN5600A-R2, or LVN5800A-R2 unit, can be deployed at each additional subnet. We understand that each network is unique. We offer free support to help you best plan out your deployment around your own network topology. Contact Black Box Technical Support at 724-746-5500 for more information.

QUESTION: I purchased a Veri-NAC Enterprise with multiple physical Ethernet ports; can I use each of these Network Interface Cards (NICs) on the same subnet?

ANSWER: Yes, as long as the IP ranges don't intersect.

QUESTION: Should each VLAN have its own device?

ANSWER: It depends on your network configuration: if the Veri-NAC can see MAC addresses, it can block. If not, place a LVN5200A-R2 or LVN5250A-R2 unit on that particular subnet and control that unit from the LVN5400A-R2, LVN5600A-R2, or LVN5800A-R2 unit with Command Center.

QUESTION: I got an alert e-mail from Veri-NAC stating that it detected a new untrusted asset, but blocking didn't happen. I can ping from that untrusted device to other PCs in the intranet. The Dynamic Detection System is enabled and the PeerBlock Blocking option is selected.

ANSWER: The Protect Range entered on the DDS page may be the issue. Let's say you're on the class C subnet 192.168.0.1/24 and the Protect Range is set to 192.168.0.40-60. This will prevent a blocked asset from being able to communicate with IP addresses within 192.168.0.40-60. Assets outside of this range, for example 192.168.0.1, will still be reachable by the blocked asset(s). In this example, set the protect range to 192.168.0.1-254 to solve this problem.

QUESTION: Does the PeerBlock clientless method block the communication between untrusted IPs and selected IPs inside the network and if so, is it a good idea to put all my LANs into both Block and Protect Range?

ANSWER: The Block Range is the range that is always blocked upon plugging in. The Protect Range causes all the IPs in its range to be invisible to the attacker. If you set the entire subnet(s) where you actually have assets, this will work perfectly. The only exception would be to set the protect range to some unbelievably large and unrealistic network scheme like a full class A network, when you might only have 100 or 1000 computers. By setting the protect range way too high, you would make far too much traffic during a block event.

2. General Use

QUESTION: How do I change the date on which Auto-Update will run?

ANSWER: Auto-Update is automatically updated daily, but you can run a manual update by clicking "Update Now." The appliance runs a Web-based secure subscription service in the background.

QUESTION: What methods of SNMP traps are supported?

ANSWER: SNMP traps, versions 1 and 2c are supported.

QUESTION: When does Veri-NAC check for new devices that connect to the network?

ANSWER: On the left menu of the Veri-NAC Web interface, go to Network Access Control→PeerBlock Blocking or Network Access Control→Manage IPs. The assets with IP addresses highlighted in red are currently being blocked.

QUESTION: How do I remove a client that is listed under "MAC IP Mismatch"?

ANSWER: Go to Network Access Control Manage IPs and, from the drop-down Manage… menu at the top left of the screen, select MAC IP Mismatch List. This will show all clients in the MAC IP Mismatch list. Select the one you want to delete.

QUESTION: Is there a way to clean out the database in Veri-NAC? I plan to travel using a unit to audit different sites, and I'd like to have old information wiped out, to prevent a difficult-to-manage information load.

ANSWER: We do not allow users to clear out the IP database for forensic/historical reasons. However, you may choose to do a factory reset, which will restore your unit to factory settings: Go to System→Utilities→Factory Settings. This will clean out everything, except the database of IPs that have been audited.

QUESTION: Why do I get a security certificate error in Internet Explorer®/Firefox®?

ANSWER: We assign the Veri-NAC certificate ourselves. Internet Explorer (IE) version 7 considers all self-assigned certificates untrusted, so you will see a certificate error message when opening Veri-NAC's login page in IE 7. You can accept and install the certificate to get rid of this error message by following these steps:

1. Ignore the warning and proceed by clicking on "Continue to this website (not recommended)."
2. Your address bar will be highlighted in red next to a Certificate Error icon.
3. Click on the Certificate Error icon to open the information window. Click on "View Certificate." Then click on "Install Certificate." You'll see yet another warning. Click on "Yes," and then you're done.

To get rid of certificate errors in Firefox:

1. On the screen that comes up when you get a certificate error, click on "Or you can add an exception.".
2. Click on "Add Exception."
3. The appliance's IP should be automatically filled in the "Server Location" field.
4. Click Get Certificate→Confirm Security Exception and you're done.

QUESTION: I keep getting this certificate error in Firefox: "(Error code: sec_error_reused_issuer_and_serial)." What can I do about it?

ANSWER:
1. Go to Tools→Option→Advanced Encryption and click on View Certificates.
2. In the Servers and Authorities tab, remove the appliance certificate by highlighting the appliance's IP and clicking "Delete."
3. Try refreshing the page and add the appliance to the exception list.

QUESTION: My updates are failing. What can I do?

ANSWER: Make sure the System Date and Time is set correctly.

QUESTION: What is the control status of PeerBlock after a power reset?

ANSWER: When Veri-NAC is power cycled, it will resume packet scanning and asset blocking upon restart if these features were enabled when the unit was powered down.

QUESTION: I am concerned about how a large number of Veri-NAC appliances can be managed centrally. For example, I have 5000+ computers in 50 segments, which means I need to have 50 devices. For Veri-NAC authentication, it seems that we have to maintain one pair of IDs/passwords for each administrator in each Veri-NAC appliance, so a total of 50 passwords need to be assigned to each staff. Manageability becomes an issue. Am I able to customize the passwords for every unit?

ANSWER: All 50 units can have the same password. Every unit has a default admin-level username called MainAccount, which is capable of making password changes. Using MainAccount, you can also add more users with admin privileges if you want.

QUESTION: Can I authenticate my PCs or desktops based on their MAC address, so that PCs or desktops whose MAC addresses are not in the database will not be granted network access?

ANSWER: Yes, Veri-NAC allows you do this. This mode of authentication requires that any new PCs or desktops connected to the network be authenticated based on this MAC address database. If the MAC address is not in the database, the new PC is not given network access.

QUESTION: When the Veri-NAC box is introduced into the network, will all assets detected be put on the untrusted list by default, during Asset Discovery?

ANSWER: No—they are all automatically trusted, unless you start the Dynamic Detection and blocking system with NO assets in the trusted asset list. We recommend turning off Dynamic Detection System first (default setting) and doing an asset discovery Network Access Control→Asset Discovery then reviewing this trust list at Network Access Control→ Manage IPs.

QUESTION: Can I set a policy to define that any "untrusted" asset can only see a few IP addresses, such as an Internet proxy IP address? In other words, I want asset exclusion to be based on IP addresses, not MAC addresses.

ANSWER: Yes, you can—easily. When an untrusted asset is being blocked, it can't see IPs that are in the defined protect range. However, it can see IPs that are not in the protect range.

For example: Let's say you want to block a contractor's laptop for access to critical servers, but this person can have access to the Internet, printers, and anything else. Assume the internal network is class C range from 192.168.1.1-254. The gateway IP address for access to the Internet is 192.168.1.1, the Veri-NAC IP is 192.168.1.9. The critical servers cluster resides from 192.168.100-110. Here is how you would set up this policy on the Veri-NAC: From Network Access Control Dynamic Detection System: Click the checkbox for "Enable PeerBlock blocking" Enter "192.168.1.1-254" in the Block Range, "192.168.100-110" in the Protect Range. Now, click "Save" at the bottom of the page.

Result: When an outside contractor plugs in her laptop, she wouldn't be able to see any of the critical servers. However, she can have access to the Internet and other non-critical servers without knowing that critical servers exist. When you are in admin view on the Veri-NAC Web interface, you will see that her laptop is being blocked (red highlight on the Manage IPs page).

QUESTION: What is the IP/MAC Mismatch list for?

ANSWER: Let's look at a sample scenario:
A network asset, PC1 has the IP address 192.168.1.183. and PC2 has the IP address 192.168.1.207. Both PCs are on the trusted list. PC1 goes offline. PC2 either statically reassigns its own IP to 192.168.1.183 or PC2 requests a new IP, and the DHCP server leases 192.168.1.183 to PC2. Veri-NAC will move PC1 to the mismatch list and give the reason "IP address unknown." The PC2 info will overwrite the PC1 data on the Manage IPs page. PC2 can access the network normally. Later, when both PCs revert to their original IP addresses, PC1 will be removed from the IP Mismatch list. You can also choose to remove IPs in the Mismatch list manually.

3. Advanced Use

QUESTION: In our network environment, ICMP traffic is blocked; does this affect the Asset Discovery function? Is Veri-NAC still able to discover the server(s)? Does the Veri-NAC appliance use only the ping packet to discover assets?

ANSWER: Veri-NAC's Dynamic Detection feature detects DHCP lease requests. If packet sniffing is enabled, the appliance will inspect network packets to detect new assets, including static IP devices.

QUESTION: What protocol does Veri-NAC use to dynamically detect assets?

ANSWER: Veri-NAC uses ping combined with other technologies to discover assets. Even when ICMP traffic is blocked, Veri-NAC will be able to discover assets.

QUESTION: If the log space on the hard disk is full, what does Veri-NAC do? Will it overwrite the old logs?

ANSWER: System Statistics shows disk usage. It will give warnings when the disk is at least 75% full. However, we recommend frequent backups, because Veri-NAC will overwrite old logs if necessary.

QUESTION: What is the amount of bandwidth difference between the low bandwidth probe and normal bandwidth probe?

ANSWER: The appliance contains a "smarter scanning engine" that manages bandwidth usage automatically. If an audit has six or fewer IP addresses being audited at the same time, it will run in low bandwidth mode, using approximately 20 kbps. If an audit has more than six IP addresses being audited at once (this could include dozens, hundreds, or even thousands), it will throttle up to high bandwidth mode, but never go over 140 kbps network usage (on average).

QUESTION: Does Veri-NAC authenticate MAC addresses and block MAC spoofing?

ANSWER: Veri-NAC does provide MAC spoofing detection and blocking. If two or more devices are on-line at the same time, you will receive an e-mail, and you can have them blocked on detection.

QUESTION: What technique is used to block unknown computers and other devices? Does it affect performance in a "busy" end user network?

ANSWER: The appliance uses a patented methodology to block untrusted devices from getting on the network. Generally speaking, it is confusing the untrusted asset by feeding it wrong information and creating a low-bandwidth denial of service using PeerBlock, or through rule changes on Managed Switches (Black Box part number LGB1002A-R2, LGB1003A-R2, or LGB1005A-R2) and firewalls. PeerBlock uses 7 kbps of bandwidth to block, network activity whatsoever. "Normal conditions" means only a few untrusted assets at a time, not an abnormal situation, such as 100 untrusted assets simultaneously attempting to access a small network. The stream of only 7 kbps to block unwanted users is very little bandwidth usage. That's the most bandwidth usage per IP blocking event the appliance will use. Network traffic generated while Veri-NAC is auditing or vulnerabilities ranges from 40 to 120 kbps, therefore, is almost invisible to users even while it discovers their common vulnerabilities and exposures. However, there are some dos and don'ts we recommend to make traffic smooth and invisible. These are covered in the README FIRST! document you received with Veri-NAC and include not auditing a critical overloaded server during busy work hours and dealing with alerts from intrusion detection systems (IDS).

QUESTION: Is MAC addressing the criteria for blocking unknown devices and if so, what if I move the Ethernet NIC to another computer?

ANSWER: Yes, that is the criteria. So if you move the NIC to another computer, you will be triggering the MAC spoof detection mechanism. Run Asset Discovery to update the Veri-NAC database.

QUESTION: Does the Veri-NAC appliance have a guest policy in which guest computers can only access the Internet, not the internal network?

ANSWER: Yes. Veri-NAC has a Protect Range feature—anything in the range is going to be invisible to the untrusted asset. Any exclusion in the range will be visible. For example: if you exclude a router that leads to the Internet, the untrusted asset will think there is only one asset on the network and communicate with it. That router will provide access to the Internet while other peer devices are "invisible" to the guest.

QUESTION: How does Veri-NAC deal with internal threat propagation? How does the appliance identify and quarantine the endpoint?

ANSWER: Veri-NAC has the capability to preemptively block the vulnerable asset or port at the Managed Switch (for example, Black Box part number LGB1002A-R2, LGB1003A-R2, or LGB1005A-R2 and firewalls). It handles malware more proactively through starvation—eliminate the vulnerability, and you become more immune to exploits. Finally, if a system is propogating malware, in real-time, remove it from the trust list and make sure the PeerBlock engine is enabled. This should kill the malware propogation and data leakage risk from the infected endpoint.

QUESTION: Is it possible to provide a Web page forwarding the unhealthy endpoints to remediation facilities?

ANSWER: There's really no good automated way to fully remediate an unhealthy system, yet. We recommend that you fix the vulnerabilities by patch or system reconfiguration instead of sending users to Web pages.

QUESTION: Can I administer and consolidate an asset list across multiple appliances?

ANSWER: Currently Veri-NAC appliances do not share their asset lists between each appliance, however, you can access and control these asset lists from a single appliance running the Command Center.

QUESTION: Cisco also has MAC authentication control at the Managed Switch port layer. How does Veri-NAC compare
with Cisco's solution?

ANSWER: In testing, we have found that a $20 hub can render Cisco's solution ineffective. If you place a small, low-cost hub on the subnet, the untrusted MAC address device is still able to attack and eavesdrop on its peers across the hub. Also, Cisco's 802.1x methodology is costly, requires complete infrastructure upgrades, and is frequently hacked. Veri-NAC also offers the ability to communicate with Cisco Managed Switches, even the older Catalyst, using a simple block methodology.

QUESTION: How does the Veri-NAC appliance detect when a PC or laptop is connecting to the network?

ANSWER: It uses static IP Detection (at the ARP event level) and DHCP Detection (at the IP Broadcast event level).

QUESTION: How does Veri-NAC block PCs or laptops that are not authenticated?

ANSWER: The Veri-NAC appliance uses three layers of blocking, depending on which you choose to use—firewall rules change, Managed Switch port bloc,k and, our favorite, PeerBlock blocking which uses a lightweight ARP-level packet-blocking engine running a low bandwidth 7 kbps per untrusted asset during a block event.

QUESTION: Can Veri-NAC appliance integrate with the CA-Unicenter®, HP® OpenView®, or IBM® Tivoli®?

ANSWER: Yes. These information management systems accept both Syslog and SNMP traps, so you can consolidate alerts from one or more Veri-NAC appliances into one console.

4. Managed Switches and Firewall

QUESTION: What kind of Managed Switches does Veri-NAC send quarantine information to, as an optional blocking method?

ANSWER: Under Managed Switch quarantine, there are dropdown selections for the Managed Switches the appliance can communicate with, which is not required for PeerBlock quarantine, they are 3Com®, HP®, Extreme Networks, Cisco™, and Black Box (Black Box® part numbers LGB1002A-R2, LGB1003A-R2, or LGB1005A-R2) Managed Switches.

QUESTION: When Dynamic Detection is enabled, newly connected devices are blocked as they connect. Why is this happening?

ANSWER: Depending upon how you configured the appliance, as each new, untrusted device connects, a rule blocking that device is created automatically.The Veri-NAC will block using three optional methodologies:

a. Block at the firewall (if supported)
b. Block at the Managed Switch (if supported). Methods include blocking physical switch ports and 802.1Q VLAN tagging with black holing.
c. PeerBlock, by targeting a Denial of Service (DoS) at the invader on the network (this is the best, easiest way to block, using very little traffic, about one 7-kbps stream per invader).

QUESTION: How long does a Dynamic Detection-created rule on the Managed Switch or firewall remain active?

ANSWER: The rule remains as long as there is an untrusted device or port-level vulnerability. However, the admin receives an alert when the rule is created and can manually make changes to the rule if so desired.

QUESTION: When I unplug the Veri-NAC from the network, the Managed Switch or firewall seems to continue applying

standing rules created during Dynamic Detection. How can I stop this?

ANSWER: You need to delete the rules manually from the Managed Switch (for example, Black Box part number LGB1002A-R2, LGB1003A-R2, or LGB1005A-R2) or firewall. Please see the user's manual for your Managed Switch or firewall for more details.

QUESTION: Can I integrate more than one Managed Switch within the same network LAN?

ANSWER: Yes.

QUESTION: When integrating our Veri-NAC with a compatible Managed Switch or firewall, are we only required to configure Veri-NAC, or do we have to make a manual configuration on the Managed Switch or firewall as well?

ANSWER: In most cases, as long as your Veri-NAC appliance has an admin access to and can successfully communicate with the Managed Switch (for example, Black Box part number LGB1002A-R2, LGB1003A-R2, or LGB1005A-R2) or firewall, there is no need for manual configuration on the Managed Switch or firewall. However, each firewall has different rules. The Veri-NAC user guide explains how to set up your firewall to be compatible with Veri-NAC. Using the Juniper Networks® NetScreen® firewall, for example, you first log into the firewall and make/delete a rule. The Juniper firewall won't allow remote rule creation without first doing this once. Other firewalls do not require this step. However, if you tell a firewall by default to only allow, say, IP address 192.168.254.2 to log in, and your Veri-NAC is at .3, then it will block your Veri-NAC from remotely (SSH/TELNET/API) connecting in, even if you have the user ID and password. Make sure Veri-NAC is on the "allow" list of firewall admin users.

QUESTION: To use the Internet for automatic updates, I need to go through an authenticated proxy server. What is the IP address or Web site that Veri-NAC uses to update its signatures and patches, so that I can configure my firewall accordingly?

ANSWER: The appliance connects to https://ssl.perfora.net/updateauditor.com for its updates. The outgoing ports used by the appliance vary; however, the starting port number the appliance will use is 36280. The incoming port used by the server is 443. The protocol is https. The proxy setting can be created or modified by going to System Proxy Configuration.

QUESTION: What protocol is used between Veri-NAC and a Managed Switch (for example, Black Box part number LGB1002A-R2, LGB1003A-R2, or LGB1005A-R2) or firewall?

ANSWER: SSH or TELNET.

QUESTION: Does Veri-NAC work on all Managed Switches? Are any configuration changes required on the Managed Switches?

ANSWER: If the only feature in use is PeerBlock blocking, Veri-NAC is compatible with all Managed Switches. If the Managed Switch

blocking feature is in use as well, then access to the Managed Switch via Telnet/SSH will be required. Our currently supported Managed Switches are Black Box part numbers LGB1002A-R2, LGB1003A-R2, and LGB1005A-R2; Cisco; 3Com; Extreme Networks; and HP.

QUESTION: Can Veri-NAC integrate with the Check Point firewall?

ANSWER: Yes, it works with the Check Point® firewall.

QUESTION: Does Veri-NAC work with the Alcatel Managed Switch or the Cisco ASA Firewall?

ANSWER: It does not currently integrate directly with these models. Use the PeerBlock blocking feature, which will work independently of any Managed Switches or firewalls regardless of type.

5. Audits

QUESTION: **When I try to edit previously scheduled audits, I can only delete them. They are not underlined and are not available for edit. Is this a bug or a feature?**

ANSWER: This is a feature, not a bug. You have to stop a scheduled audit before you can edit it if it is "running," that is, scheduled. Press the Stop button. Even though it's not running now, you will be able to edit it.

QUESTION: **What is the impact of Veri-NAC on the performance of a network during the auditing process? Will it slow down the network or network-based applications and servers we are running?**

ANSWER: The appliance has minimal to no impact on network performance or bandwidth, with a few exceptions: Although Veri-NAC performs non-invasive network asset probing and Common Vulnerabilities and Exposures inspection, make sure you don't audit a critical server during a critical time the very first time you use the appliance. First, auditing your DNS server during working hours is not recommended. Auditing an Intrusion Detection System (IDS) is also not recommended, as the IDS might think that the Veri-NAC appliance is a "hacker" and send out network alerts that are false positives. In addition, Symantec Antivirus software for Microsoft Exchange acts like an IDS on your mail server, so you have to be very careful if and when you audit this system. The same holds true for your firewall, VPN, and other information security countermeasures, which send alerts when they are probed for information. You may be able to add Veri-NAC to a trust list so it is not perceived as an "insider" threat on your networks when auditing these security systems. Second, make sure that, when you log into the appliance for the very first time, you click Updates→Vulnerabilities→Signatures→Update Now to make sure your appliance has the latest CVE tests. Third, make sure that you have the newest service pack installed on Veri-NAC system by following Updates→Service Packs→Install Patches. Finally, the bandwidth usage is as follows on a Class C network (or larger): No more than 100 kbps/no less than 40 kbps during a full audit. No more than 7 kbps per PeerBlock block session against a single untrusted asset (if PeerBlock is blocking, the asset will be inaccessible).

QUESTION: **Some Intrusion Detection Systems (IDS) and Host-Based Intrusion Detection Systems (HIPS) detect when they are being audited and think it is a hacker or a port scanner. How does the Veri-NAC bypass this detection?**

ANSWER: Some HIPS and IDS are able to detect the Veri-NAC activity as a port scan. Veri-NAC is doing a port scan along with more detailed analysis of CVEs. Whenever possible, configure HIPS and IDS to allow the Veri-NAC traffic as an exception, without escalation and alerting.

QUESTION: **How does Veri-NAC handle licenses for a virutal environment? For example, if I have 10 different servers' operating systems (OSs) or applications running within a virtual server, such as VMware, all on one piece of physical computer hardware, what license would be required to audit all the applications or operating systems?**

ANSWER: Unfortunately, the current release of Veri-NAC does not consider a virtual OS with the same MAC address a different "virtual" computer and would treat it as a MAC/IP mismatch for NAC purposes, and CVE auditing results would vary.

QUESTION: **How do I quickly stop all currently running/scheduled audits?**

ANSWER: Navigate to System Utilities and select "Stop All Audits."

QUESTION: **Under Audits→View Vulnerability Tests, only Windows® and Linux® operating systems are shown. What about other devices and operating systems, such as printers, VoIP phones, etc?**

ANSWER: These groupings allow you view tests relevant to these operating systems. To view all tests, select "All OS."

6. Workflow/Ticket Management

QUESTION: **Can the workflow engine be automated so vulnerabilities are automatically fixed?**

ANSWER: Fixing CVEs is not as simple as running patch updates in most cases. Some remediation of vulnerabilities can be done with patches, many require fixing configuration issues, and some require upgrades. In addition, it is essential that CVEs are remediated correctly, as incorrect patches and configuration changes can cause more problems and troubleshooting issues. It is best to do system hardening manually.

QUESTION: **An audit discovered one particular vulnerability ID that is located across 100 PCs on my network. As far as I can see, I can only assign the task of fixing these 100 PCs to one person, which may take a long time. Would it be possible to assign groups of those 100 PCs to different IT staff users? For example, one staff member gets a task of 50 PCs, and another staff member takes care of the other 50?**

ANSWER: Yes. Assign this job to an IT staff user first, and then reassign it to multiple persons using the Workflow/Reassign Tickets menu.

QUESTION: **There are some jobs that I cannot close. They show up as "N/A" in my menu.**

ANSWER: This is because a staff member is working on a job ticket containing more than one vulnerability. A manager can assign more than one vulnerability ID (VID) to an IT staff using one Job Ticket Number. For example, the manager can assign ub-task VID 22222 (risk level: serious) and VID 10397 (risk level: low) as Job Ticket #1. An IT staff member will then work on these sub-tasks serially in order of their risk level. In this case, he must work on VID 22222 first, then VID 10397. While he's working on VID 22222, the Start Date, Complete Date, and Comments columns for VID 10397 will display as "N/A."

QUESTION: **I assigned one VID to one IT staff member. Why do some of the Report Tickets that have same Vulnerability ID have the value of 2 and 3? Shouldn't the number be "1," because it is only 1 ID assigned?**

ANSWER: Workflow counts the number of vulnerabilities and number of tasks differently. Using your example, if you click the link of the Report Ticket for this newly assigned VID, under column IP (Report Ticket), you will see there are two vulnerabilities for Report Ticket #38 and #33, and three for Ticket #21. That's because this VID is found at two IPs for Report Ticket #38 and #33, and three IPs for Ticket #21.

QUESTION: **There is a disparity between the numbers reported under the "Unassigned" header in "Workflow Ticket Log" and the actual number of unassigned tasks. For example, the number of unassigned tasks reported may be 6, but when I click the link to view details, I may find only 5 unassigned tasks. Is there a problem?**

ANSWER: If the same vulnerability (VID) is found at two different IPs, the Veri-NAC reports them as two vulnerabilities, while Workflow counts them as one task (because they have the same VID). Workflow counts number of vulnerabilities and number of tasks differently. When you click to view details, you see 5 unassigned tasks, but if you look at the IP (Report Ticket) column, you will find 6 vulnerabilities for this Report Ticket.

QUESTION: How do I keep track of vulnerabilities that have been fixed?

ANSWER: Go to Workflow→My Ticket Log→View MainAccount's Closed Jobs. You can then see the detailed information of the closed jobs for MainAccount.

QUESTION: While running the Veri-NAC system, I found managing and tracking vulnerabilities to be somewhat difficult. As the sole user of the device, it is difficult for me to add comments to a report and then move it to different stages "to be determined" and "closed". Although I am the sole user of the device, I can't simply do these things myself, having instead to log on as the system administrator if I wish to move an issue on to the next stage. Also, is there a way for me to reopen and modify a job which has already been closed?

ANSWER: Workflow is designed in such a way that only an administrator, not an IT staff member, can close a job. Unfortunately, after a job is closed, no changes can be added, but you can view the history of any closed job at My Tickets Log. You can make yourself an administrator of the appliance by logging in as MainAccount.

QUESTION: When does the Veri-NAC check if jobs are past due?

ANSWER: Twice a day (8:00 A.M. and 12:00 P.M.). If it finds jobs past due, it then sends an e-mail to the IT manager(s) for escalation.

QUESTION: Why can't I close the ticket of the job I just completed?

ANSWER: Only your manager or MainAccount can close your job ticket. Even Manager-level users cannot close tickets for jobs they are assigned to.

QUESTION: One of my staff members went on vacation, and she still has open job tickets assigned to her in Workflow. Can I reassign her tickets to other staff members?

ANSWER: Yes. Go to Workflow→Reassign tickets and follow the steps. You may want to consult the Veri-NAC user's manual. Please look in Section 16.8, Reassigning Jobs.

QUESTION: Can I assign multiple resources for an individual job?

ANSWER: Yes. Go to Workflow→Reassign tickets. Select the job number you'd like to reassign. On the next page, select any amount of resources you'd like (use the CTRL key when selecting), adjust the assigned man hours as needed, then click "Continue."

7. Policies, Regulations, and Reports

QUESTION: Why am I unable to upgrade the ISO 27001/17799 Policy? The selection button is grayed out.

ANSWER: If you already have the policy tool installed, then no upgrade is available. Go to the Policies and Regulations→ ISO 27001/17799. If this opens a spreadsheet, you are fine. If not, call Black Box Technical Support at 724-746-5500.

QUESTION: What is the purpose of the "Open Vulnerabilities" and "New Vulnerabilities" graphs in the "Trend in Vulnerability Status" section of a Management or Executive report?

ANSWER: An Open vulnerability is a vulnerability that is listed in Workflow tickets and has not been resolved.
A New vulnerability is a new CVE in the Workflow database.
An example in Executive/Management Report:
Currently open vuls*: 36
Fixed vuls: 20
Total Discovered vul =currently open vuls + Fixed vuls = 56
New vuls: 8* vul = vulnerability

QUESTION: I fixed all vulnerabilities present in my job tickets and then generated a report. Despite all vulnerabilities being fixed, the "Fixed Vulnerabilities Graph" does not match the "Total Discovered Vulnerabilities." The graphs seem to indicate that there are still open vulnerabilities. If I look at the report, it says that the jobs are closed and all vulnerabilities are fixed.

ANSWER: Even though the job status for this vulnerability is set as "fixed," the Veri-NAC doesn't consider it to be. You should to run an audit again to ensure that this vulnerability is really fixed.

QUESTION: Once I complete a policy in Basic Policy Builder, is there a way to print out the policy that I created so I can keep a hard copy?

ANSWER: Yes. Go to File Print or press CTRL-P on your keyboard. To ensure your policy is what gets printed, make sure this window is the highlighted browser window—click inside the final policy window with the mouse to be sure, then press CTRL-P.

QUESTION: Basic Policy Builder lists 26 default policies; is there a way to create a new policy other than those 26 items (creating policy 27, 28, and so on)?

ANSWER: Unfortunately, in the present version you cannot create a new policy. However, feel free to open up Microsoft Word, copy your final policies into a Word document, and then begin editing your new policies 27, 28, and so on.

QUESTION: How does Veri-NAC know if my network is in compliance with ISO 27001 for reporting purposes?

ANSWER: Veri-NAC tests for Common Vulnerabilities and Exposures (CVEs) which could cause a breach of Confidentiality, Availability, and/or Integrity (CIA), which would create the risk of being out of ISO compliance. Knowing that your network is free of CVEs eliminates this particular compliance risk. Also, the ISO 27001/17799 policy builder tool included with our larger enterprise appliances helps companies to audit, test, and build ISO-compliant policies that are corporate wide and out of the core scope of the appliance but fully ISO 27001 compliant.

QUESTION: Is Veri-NAC compatible with the Committee on Payment and Settlement Systems?

ANSWER: Veri-NAC is compatible with the Committee on Payment and Settlement Systems (CPSS), but it does not guarantee that transactions are secure. By detecting and removing CVEs that could breach CIA, as well as using our best-practices ISO 27001 and basic policy tools, you can show steps of due care and due diligence for CPSS.

QUESTION: Does my company's logo only show on first page of a report?

ANSWER: Yes, the logo appears only on the report's first page, while your company name and address is on the bottom of every page.

QUESTION: When I view an audit report, it reads "The remote host is not available, so it cannot be audited." I have checked to make sure the machine is turned on. Why can't I audit that machine?

ANSWER: Make sure any local host-based software firewalls running on that machine are turned off before running an audit.

8. Backup and Restore

QUESTION: Does Veri-NAC appliance have a backup and restore facility?

ANSWER: Veri-NAC does have backup/restore capability. Please see documentation on System Backup and Restore.

QUESTION: Can I change the name of the file that is created during a backup?

ANSWER: No, do not do this. The file will then be unrecognizable to Veri-NAC should it need to run a restore.

QUESTION: Do I need to delete the backup file from Veri-NAC?

ANSWER: It is not required, but we recommend doing so to save hard drive space.

QUESTION: After I perform a restore on Veri-NAC, will my updated patches be restored back to the earlier version?

ANSWER: No. Only the data and configuration information reverts to the former state. Please make sure you keep track of all login IDs and passwords—new and old. You might need this to log back in.

QUESTION: What is included in a Backup/Restore?

ANSWER: The Veri-NAC appliance will back up the following:
Reports and Workflow
Audit Configurations
Asset Tracking Data
Veri-NAC appliance Settings
Veri-NAC appliance Log(s)

QUESTION: I use a Linux®/Unix® File Server. When I back up the system in the "Backup and Restore" section, is my Linux username and password required since to write files to the OS, I need to use my username and password to grant permission?

ANSWER: See Backup and Restore in the Veri-NAC User Guide:
From System Backup and Restore, click Change Backup Settings.
Click "Important steps required" for Linux servers to work.
Follow the provided instructions. If you have questions, call Black Box Technical Support at 724-746-5500.

9. Command Center

QUESTION: What is the Command Center?

ANSWER: The LVN5400A-R2, LVN5600A-R2, or LVN5800A-R2 Command Center offers the ability to command and control remote

Veri-NAC appliances across our network. Remote appliances can be added, and groups of remote appliances can be created. In one action, policies and configurations can be saved to all remote appliances included in a group.

Remote actions can be performed on remote appliances. Group and appliance status can be quickly viewed on a single screen, providing an easy-to-use management console.

QUESTION: I am planning a project for a large network; I need to understand more about manageability so I can be confident when it goes into operational mode. Can you please share with me the operation/deployment model Veri-NAC has used for large-size customers?

ANSWER: Management can be either local (console) or remote (https). The units can be grouped and managed remotely from the LVN5400A-R2, LVN5600A-R2, or LVN5800A-R2 unit using the Command Center on networks of any size. It really depends upon how many VLANs, subnets, and physical locations there are. With this information, you should be able to deploy one or more Veri-NAC appliances to protect your entire network.

QUESTION: Can the Veri-NAC LVN5400A-R2, LVN5600A-R2, or LVN5800A-R2 unit with Command Center have the same trusted list database as another sub-unit?

ANSWER: Yes, it can.

QUESTION: What is the default port Veri-NAC LVN5400A-R2, LVN5600A-R2, or LVN5800A-R2 uses to communicate with managed LVN5200A-R2 or LVN5250A-R2 units and can I change it?

ANSWER: Port 443 (SSL) is the default.

You can change the port to any number you like as long as both the LVN5400A-R2, LVN56500A, or LVN5800A-R2 and all managed appliances use the same port. Don't forget to open the port on your firewall to allow traffic from the Veri-NAC LVN5400A-R2, LVN56500A, or LVN5800A-R2 Command Center to each remote Veri-NAC LVN5200A-R2 or LVN5250A-R2 unit.

QUESTION: I added a Veri-NAC LVN5200A-R2 or LVN5250A-R2 unit to my Command Center group. When I look at my managed appliances, I see a red icon next to the LVN5200A-R2 or LVN5250A-R2 unit. When I click on it, it displays the message "Appliance Unavailable." What's wrong?

ANSWER: This means the Command Center cannot communicate with that Veri-NAC unit. Please check the following:

- Is the Veri-NAC LVN5200A-R2 or LVN5250A-R2 unit turned on?
- Is the Ethernet cable plugged in properly?
- Can the Command Center receive information from the IP address of the remote unit? Make sure the LVN5200A-R2 or LVN5250A-R2 unit's IP isn't accidentally in the Block Range.
- Can the LVN5200A-R2 or LVN5250A-R2 unit be accessed locally from the browser (https)?
- Is the default port the same for both the LVN5200A-R2 and LVN5250A-R2; and LVN5400A-R2, LVN5600A-R2, and LVN5600A-R2 units?
- Did you configure the firewall or other intermediate devices to forward the SSL port traffic properly?

QUESTION: Why would I use 802.1q VLAN tagging?

ANSWER: This feature is very useful if you want to efficiently use less Veri-NAC hardware to protect a larger or more complicated network that uses VLANs. When you want to have one Ethernet port of your Veri-NAC appliance see and help manage network access and vulnerabilities in up to ten (10) VLANs per physical Ethernet connector, you simply tag all these VLANs and plug Eth0 of your Veri-NAC appliance into the physical port on your Managed Switch where you have the tagged VLANs mapped.

QUESTION: I enabled 802.1q VLAN tagging in my Managed Switch and now my network seems to have gone down. What happened?

ANSWER: Use 802.1q VLAN tagging only if you fully understand how to properly configure this feature both in your Managed Switch (for example, Black Box part numbers LGB1002A-R2, LGB1003A-R2, or LGB1005A-R2) and your Veri-NAC appliance. This feature is optional and not required to use your Veri-NAC appliance.

802.1q VLAN is a very powerful feature of your Managed Switch. If you misconfigure the physical tagged ports of your Managed Switch, the switch itself might send tagged traffic over your network causing devices to appear to lose connectivity or be offline, when they are not actually offline.

Make sure the physical Managed Switch port that you have bound to the tagged VLANs is plugged into one of the enabled Ethernet ports of your Veri-NAC appliance.

QUESTION: Why can't I open the ISO 27001 policy tool on my Veri-NAC (LVN5400A-R2, LVN5600A-R2, or LVN5800A-R2)?

ANSWER: If you open this tool using Internet Explorer®, it will open an Excel file remotely from the Veri-NAC appliance. You might have to click on an Internet Explorer popup dialog box to agree to download this content. When you do so, it should open fine. Then, if you attempt to click a hyperlink in one of the Excel® tabs from within your Internet Explorer browser, you will go through the same process to open one of the many sample policies in the Word document format. If you are using Firefox®, by default it will attempt to download the Excel spreadsheet locally. By doing so, the embedded Word document hyperlinks will not work because they are looking for files on a relative path. You will need to run this tool using Internet Explorer as your default browser.

10. New Features in Veri-NAC Version 8.0

QUESTION: What are the key new features in the Veri-NAC appliance, version 8.0 firmware update?

ANSWER: Veri-NAC now includes advanced features for Active Directory integration, improved asset manufacturer recognition, agent-less Malware Detection, VLAN restriction and allowance across multiple 802.1q enabled VLANs, improved agent-less blocking performance, and updated Auditing. It also includes Regulatory compliance support including the Payment Card Industry (PCI) standard and NERC/FERC compliance auditing, protecting and reporting for the energy/power grid critical infrastructure among others such as HIPAA and GLBA.

QUESTION: What kind of integration does Veri-NAC offer with Microsoft® Active Directory?

ANSWER: The Veri-NAC appliance now offers two components for integration with Microsoft Windows Active Directory. In one feature, Veri-NAC users can now log into the appliance using their Active Directory credentials—username and password. In another feature, it offers the ability to track login events when users gain access to the network and log into the Active Directory Domain.

QUESTION: Is the Active Directory integration between Veri-NAC and the Active Directory controller secure?

ANSWER: The connection between the Veri-NAC appliance and the Domain Controller is a secure connection and requires a certificate to be installed on the Domain Controller and a tiny piece of 'service' software to be installed. Please refer to Microsoft Documentation for instructions on certificate installation.

QUESTION: What versions of Microsoft® Windows have you tested this Active Directory integration with?

ANSWER: Active Directory integration has been tested with Microsoft Windows 2003 and 2008 Domain Controllers.

QUESTION: How do you track Users logging into my network?

ANSWER: In the Manage Assets page on the appliance web-based console, you will see not only the basic fingerprint of a device—such as IP address, MAC address, Operating System, Hostname—but you will also now see the Active Directory login information.

QUESTION: What are the methods for tracking User login?

ANSWER: There are standard event IDs in windows. The Windows 2003 event id being tracked is 672. The Windows 2008 event id being tracked is 4768. There are 2 methods available for tracking login events:

a) the Veri-NAC appliance provides a downloadable Windows agent. The agent installs on the Windows Domain Controller and runs as a service. The connection between the agent and Veri-NAC appliance is a secure SSH connection,

b) SNMP Traps configured on the Windows Domain Controller can pass login events to the Veri-NAC appliance. This method requires no installation of an agent on the Windows Domain Controller. Please note at time of this writing Microsoft Windows only supports SNMP V1 and V2. Please note, while no passwords are transmitted in the traps, it may be possible for the login event trap to be deciphered on the network.

QUESTION: How does Veri-NAC detect and quarantine malware infected systems?

ANSWER: Using ETH1, the 2nd Ethernet controller on your Veri-NAC appliance, you can dedicate it to sniffing for malware traffic by plugging it into a SPAN port on a switch or on a Black Box Network Tap (nTap) device that is plugged into your firewall or network router. Then, the appliance examines network traffic to determine if a network asset attempts to contact a known malware site to 'phone home' or 'download a droplet' or 'upload' internal information—typical features of malware. The system will be quarantined and you will receive an alert. Please refer to your switch vendor's documentation for instructions on monitor port setup. Refer to your network tap vendor's documentation for instructions on network tap setup.

QUESTION: How often do you update the Veri-NAC malware/threat signatures for new and zero-day malware?

ANSWER: The Veri-NAC appliance will connect to the malware/threat signatures updates service and download updates every three hours.

QUESTION: I have an infected system and it seems like Veri-NAC ignored it and didn't block it?

ANSWER: Veri-NAC's agent-less malware detection and quarantine works in conjunction with the Asset Detection System's packet sniffing. Assets within the packet sniffing range will also be scanned for malware when malware detection is enabled. Assets not within the sniffing range will not be scanned for malware. Assets within the Veri-NAC block range that contain malware that Veri-NAC detects will be blocked.

QUESTION: Should I get rid of my anti-virus software from other vendors if I'm using Veri-NAC's malware detection and quarantine feature?

ANSWER: No—keep your existing anti-virus solution. This malware feature in Veri-NAC augments your existing anti-virus system and focuses on the newer, harder to detect malware infections. Consider this a complementary feature.

QUESTION: What if one of my systems is infected and quarantined but my current anti-virus solution can't remove the infection?

ANSWER: Obtain the Data Recovery Engine (DRE), deployed on a USB stick from Black Box at http://www.blackbox.com/go/dre. It will remove the malware and salvage critical data files or save the entire system from having to be wiped and re-imaged, before you allow it back onto your network.

QUESTION: What is the Malware Whitelist in Veri-NAC and why would I use it?

ANSWER: When the Veri-NAC appliance blocks and quarantines a trusted asset that has a malware infection, it detects the public internet address that this device was attempting to communicate with. If for some reason, you feel this is a 'false positive' and/or that the public IP address should not be blocked, you can move it to the Malware IP White List.

QUESTION: Can I turn off Malware scanning and quarantining and just block untrusted devices from coming onto my network?

ANSWER: Yes. You can still use the core Veri-NAC blocking methods to quarantine and block untrusted or malicious insider access to your network, while disabling the Malware feature.

QUESTION: Let's say I am certain a site (for example, 206.18.18.120) is a malware site full of infections and I want to keep my employees safe from getting these infections. Could I manually add this site to the Malware blocking engine if I know the IP address of of the website or IP address that is deploying malware?

ANSWER: Yes. You can manually add the IP address of the bad malware site and write a short description of this mal-location. This will cause someone to be quarantined when their computer is attempting to connect to this site.

QUESTION: Can I have a Guest VLAN for Guests and keep them off other VLANs automatically?

ANSWER: Yes. The Veri-NAC appliance now offers not only this feature—the ability to restrict assets to a single VLAN but also, using the 802.1q VLAN tagging protocol, you can create a list of VLANs and allow Guests on the Guest VLAN plus employees on one or more VLANS, automatically. If they attempt to access one of the VLANs that they don't have permission to access, they will automatically be blocked and you will receive an alert notifying you that they attempted access to a restricted portion of your network.

QUESTION: Can I have trusted employees gain access to more than one VLAN but restrict certain VLANs from them for business reasons?

ANSWER: Yes. Let's say you have a EMPLOYEE VLAN, a MARKETING VLAN and a HUMAN RESOURCES VLAN. You can now Manage Assets, drill down on the target asset, such as the employee's laptop or desktop computer and set its restriction to only access EMPLOYEE VLAN and MARKETING VLAN but not HUMAN RESOURCES VLAN, if they are an employee in the marketing department, for example. You can configure this feature for each employee through Manage Assets in any way you want that matches your Managed Switches' tagged VLANs and business access rules.

QUESTION: Why is a trusted employee's laptop showing up in RED on the Manage Assets screen and they are complaining that they are being blocked from getting on the network?

ANSWER: Either they have a malware infection and are being quarantined or you forgot to trust their device or you chose to block them on purpose by removing them from the trust list or they are on a VLAN that you did not give them permission to access.

QUESTION: Why did you set a Veri-NAC block restriction default value to 3 and what does this mean?

ANSWER: When three untrusted assets come online at the same time, they will all be blocked. If a fourth, fifth or sixth, etc. untrusted asset comes online you will notice they show up in YELLOW not red but the first three are in RED. This is because Veri-NAC now limits how many simultaneous block events can occur at the same exact time. Have you ever had more than three (or the new upper limit of five) criminals or malicious insiders or untrusted people on your network at the same time? If so, there is a serious problem beyond what Veri-NAC can do to help you—most likely a major emergency. Setting this new default to three will actually protect you from making a big mistake—accidentally blocking TRUSTED employees all at the same time, which has happened enough to warrant this feature.

QUESTION: I've been having network problems, I want to narrow it down and I think I would like to totally factory reset the Veri-NAC appliance. I accidentally blocked myself, what can I do?

ANSWER: You can go to another person's computer, login to Veri-NAC and unblock yourself by re-adding your 'untrusted' asset to the trust list. If you can't get to the Web interface, you can use the Keyboard and Monitor connections directly on Veri-NAC and turn off the block engine to solve this problem. You can also choose to factory reset the appliance from here. Remember, by doing so, you will lose information so make sure you do frequent Backups, which are easy to do using the Backup/Restore feature under the System menu of your Veri-NAC appliance.

11. Troubleshooting the Veri-NAC Blocking Engine

To test to see if Veri-NAC's agentless blocking engine is working, follow these steps:

STEP 1: Start with a baseline. Disable the Asset Detection System to ensure that all blocking has stopped.

STEP 2: Make sure all assets are trusted. Go to the Manage Assets page, look for any device in YELLOW, and click on the checkbox on the left side, then scroll back to the top and Add to Trust List, which will then turn the color of that device/asset to WHITE.

STEP 3: Start with the most basic configuration. Enable Option 2 of the Asset Discovery System. You can also click on the Advanced highlighted text to open up the details policy page of the Asset Detection System and then Modify/Limit the PROTECT RANGE to only one (1) asset on the Manage Assets list (for example, 192.168.0.1-1).

STEP 4: Start the Asset Detection System. Click on the Enable Asset Detection System button.

STEP 5: Test the Veri-NAC blocking. Initiate a block against one asset. Go to the Manage Assets page and mark one asset as UNTRUSTED. This should be any asset that is online right now and not the one you put in the PROTECT RANGE. This will help you determine if the Veri-NAC appliance is able to "find" the asset and continue blocking it.

STEP 6: Verify that the asset is being blocked. This is indicated by the asset showing as red on the Manage Assets page. The row color is changed to red while there is a process running that is responsible for the blocking of the asset. Try to verify that the asset remains blocked for 20–30 seconds.

STEP 7: If the asset does not appear to be blocked, go back to Step 1 and Step 2. When you get to Step 3, disable "Check Alive."

STEP 8: Attempt to PING the asset in the protect range from the asset that is currently being blocked. You should NOT be able to reach this asset from a PING by the "untrusted" asset being blocked.

STEP 9: If you still think the block is unsuccessful, make sure the asset you are blocking cannot get on the internet or your corporate network using an alternative means (a secondary NIC or wireless card, a connection to a cellular service, etc). If you still are unable to block the asset, then your Veri-NAC appliance is misconfigured, most likely under SETUP and VLAN Configuration, it is routed away from this asset you are attempting to block, firewalled in a different network segment, or not properly gaining network access on that network segment. You should check the Ethernet connectors and the SETUP of the Network Configuration. You must use valid a VLAN, a free IP address that is valid, a network mask that is valid as well, if you are using 802.1q VLAN tagging. You must also properly configure the Gateway and DNS configurations and not put a false secondary DNS server in the ETH0 Network Configuration.

STEP 10: If none of the above is working for you, then you have a serious problem and there might be a hardware failure on some aspect of the Veri-NAC appliance. If so, please contact Black Box Support at 724-746-5500 or info@blackbox.com.